UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/819,509	03/28/2001	Mahfuzur Rahman	MATI-202US	4790

23122 7590 07/25/2005

RATNERPRESTIA
P O BOX 980
VALLEY FORGE, PA 19482-0980

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/819,509	RAHMAN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

Response to Arguments

2. Applicant's arguments, see pages 2-7, filed 24 January 2005, with respect to the rejection(s)of claim(s) 1-20 under Baird, III et al. have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Leslie Lamport, "Password Authentication with Insecure Communication" and Brown et al. (US Patent No. 6,618,806).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leslie Lamport, "Password Authentication with Insecure Communication" in view of Brown et al. (US Patent No. 6,618,806).

Regarding claims 1 and 16, Leslie Lamport, "Password Authentication with Insecure Communication", discloses the invention substantially as claimed because it teaches a one-time mechanism for countering an attack based on eavesdropping of network connections to get login id and a password. (See pages 770-771)

However, Lamport's one-time password mechanism does not teach a mechanism that obtains biometric data from a user combining the biometric data and the one-time password to form a strong password.

Brown et al. on the other hand teaches a biometric user authentication method and system wherein biometric data is obtained and is combined with a password to authenticate a user. (See Column 3, lines 21-25, 51-67)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have Lamport's one-time password mechanism implement biometric data combined with a password according to Brown et al.'s biometric user authentication system, thereby forming a strong password which authenticates a user and provide secure communication.

Regarding claims 2 and 17, Lamport in view of Brown et al. discloses the claimed limitation wherein comprising the step of encrypting the combined one-time password and biometric data using an encryption key to form the strong password (See Lamport, pages 770-771; Brown et al., Column 4, lines 16-24)

Regarding claims 3 and 18, Lamport in view of Brown et al. discloses a method and computer program for controlling access to secure data comprising the data from a user, separating the one-time password and the biometric data, comparing the one-time password and the biometric data, comparing the one-time password to a calculated one-time password to determine if the one-time password is valid, determining a probability that the biometric data is from the user, encrypting the secure data using an encryption key to obtain encrypted data if the one-time password matches the

calculated one-time password and the probability that the biometric data is from the user exceeds a predetermined threshold value, combining the strong password, the encryption key and the encryption data, and transmitting the combined strong password, encryption key and encrypted data to the user (See Lamport, pages 770-771; Brown et al., Column 5, lines 3-35)

Regarding claims 4 and 19, Lamport in view of Brown et al. discloses the claimed limitation wherein the step of encrypting the combined strong password and encryption key using a further encryption key (See Lamport, pages 770 and 772).

Regarding claims 5 and 20, Lamport in view of Brown et al. discloses the claimed limitation wherein the secure data includes items having respectively different security levels, and the step of encrypting the secure data aborts the method if either the one-time password does not match the calculated one-time password or the probability that the biometric data is from the user does not exceed the predetermined threshold value (See Lamport, page 771; Brown et al., Column 5, lines 37-54, Column 8, lines 25-50).

Regarding claim 6, Lamport in view of Brown et al. discloses a system for implementing secure access to a remote computer system comprising: at least one first computer securely coupled to the remote computer system, at least one second computer coupled to the at least one first computer and configured to obtain identifying information from a user, whereby the second computer passes the identifying information to the first computer, the first computer passes the identifying information to the remote computer system and the remote computer system verifies the identifying information (See Brown et al., Column 2, lines 11-26)

Regarding claim 7, Lamport in view of Brown et al. discloses the claimed limitation wherein the identifying information is a strong password including a one-time password and biometric information (See Lamport, pages 770-771; Brown et al., Column 4, lines 16-24)

Regarding claim 8, Lamport in view of Brown et al. discloses the claimed limitation wherein the identifying information is encrypted with an encryption key (See Brown et al., Column 8, lines 7-24)

Regarding claim 9, Lamport in view of Brown et al. discloses the claimed limitation wherein the second computer is securely connected to the first computer by means of a Secure Socket Layer connection (See Brown et al., Column 7, lines 32-42)

Regarding claim 10, Lamport in view of Brown et al. discloses the claimed limitation wherein the second computer includes a further Secure Socket Layer connection for receiving the identifying information from the user (See Brown et al., Column 7, lines 66-67, Column 8, lines 1-24)

Regarding claim 11, Lamport in view of Brown et al. discloses the claimed limitation wherein the remote computer includes firewall software through which the first computer is coupled to a remote computer (See Brown et al., Column 6, lines 27-45, 62-67, Column 7, lines 1-2, 55-65)

Regarding claim 12, Lamport in view of Brown et al. discloses a method of allowing access to secure data on a remote computer including the steps of: receiving a request from a user to access the secure data at a first computer, transferring the request to access the secure data from the first computer, transferring the request to

access the secure data from the first computer to the second computer, transferring the request to access the secure data from the second computer to the remote computer, authorizing access to the secure data at the remote computer, transferring the secure data from the second computer to the user without using the first computer (See Brown et al., Column 2, lines 11-26, Column 3, lines 6-67)

Regarding claim 13, Lamport in view of Brown et al. discloses the claimed limitation wherein the request to access the secure data includes a strong password and the steps of: encrypting the secure data with an encryption key, combining the encryption key with the strong password, encrypting the combined encryption key and the strong password with a further encryption key and transferring the encrypted combined encryption key and strong password and the encrypted secure data to the second computer (See Lamport, pages 770-771; Brown et al., Column 5, lines 3-35)

Regarding claim 14, Lamport in view of Brown et al. discloses the claimed limitation wherein the step of encrypting the combined password and strong password with an asymmetric encryption key (See Lamport, page 772).

Regarding claim 15, Lamport in view of Brown et al. discloses the claimed limitation wherein the steps of: separating the one-time password and the biometric information, comparing the one-time password to a calculated one-time password, determining a probability that the biometric information matches an authorized user and authorizing access to the secure data only if the one time password matches the calculated one-time password and the probability that the biometric information matches

an authorized user exceeds a predetermined threshold value (See Lamport, pages 770-771; Brown et al., Column 5, lines 3-54)

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Cohen (US Patent NO. 6,356,941) discloses a method and system for network vaults. Kausik et al. (US Patent No. 6,263,446) discloses a method and apparatus for secure distribution of authentication credentials to roaming users. Ballard et al. (Pub No. 2003/0225693) discloses a biometrically enabled private secure information repository. Gouric (WO 03/06341A1) discloses a two-factor authentication method with a on-time password.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CDF

cdf
July 12, 2005

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137